Thiago M. Coelho, SBN 324715
thiago@wilshirelawfirm. com
Robert J. Dart, SBN 264060
rdart@wilshirelawfirm. com
Jesse S. Chen, SBN 336294
jchen@wilshirelawfirm. com
WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd., 12th Floor
Los Angeles, California 90010
Telephone: (213) 381-9988
Facsimile: (213) 381-9989

Attorneys for Plaintiff and Proposed Class

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA – EASTERN DIVISION

TIFFANY TAYLOR, individually and on behalf of all others similarly situated,

Plaintiff,

v.

MCG HEALTH, LLC, a Washington limited liability company; DOES 1 to 100, inclusive,

Defendant.

Case No.:

CLASS ACTION COMPLAINT

1. **Negligence**
2. **Violation of CCRA**
3. **Violation of CCPA**
4. **Violation of CMIA**

DEMAND FOR JURY TRIAL

Plaintiff Tiffany Taylor ("Plaintiff"), individually and on behalf of all others similarly situated, brings this action against Defendant MCG Health, LLC ("MCG") based upon personal knowledge as to herself and her own acts, and as to all other matters upon information and belief, based upon, *inter alia*, the investigations of her attorneys.

NATURE OF THE ACTION

1. In or around December of 2021, MCG had their data servers breached by unauthorized third-party hackers, who stole the highly sensitive personal and medication information of 1,100,000 individuals across the country.[1]

2. MCG is a technology vender that provides patient care guidelines and clinical guidance software to hospitals and healthcare providers across the United States. As a result, MCG collects and stores the Personal Identifying Information ("PII") and Protected Health Information ("PHI") of hundreds of patients each day.

3. Under statute and regulation, MCG had a duty to implement reasonable, adequate industry-standard data security policies safeguards to protect patient PII and PHI. MCG failed to do so, despite specifically promising in its privacy policy that it would use "reasonable efforts to protect your information" using "a variety of security technologies and procedures to protect information from unauthorized access, use or disclosure."[2]

4. Plaintiff, individually and on behalf of those similarly situated persons (hereafter "Class Members"), bring this Class Action to secure redress against MCG for its reckless and negligent violation of their privacy rights. Plaintiff and Class Members are patients and former patients of MCG customer hospitals who had their PII and PHI collected, stored and ultimately breached by MCG.

[1] *Data Breach Notifications*, Office of the Maine Attorney General, https://apps.web. maine.gov/online/aeviewer/ME/40/ 1948d82a-0cdb-4b37-a988-b4189351176b.shtml (last visited July 28, 2022).

[2] *Privacy Policy*, MCG, https://www.mcg.com/privacy-policy/ (last visited July 28, 2022).

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

5. Plaintiff and Class Members have suffered injuries and damages. As a result of MCG's wrongful actions and inactions, Plaintiff and Class Members' names, social security numbers, medical codes, postal addresses, telephone numbers, email addresses, dates of birth and gender have all been compromised. Plaintiff and Class Members have had their privacy rights violated and are now exposed to a heightened risk of identity theft and credit fraud for the remainder of their lifetimes. Plaintiff and Class Members must now spend time and money on prophylactic measures, such as increased monitoring of their personal and financial accounts and the purchase of credit monitoring services, to protect themselves from future loss. Plaintiff and Class Members have also lost the value of their PII and PHI.

6. Further, Defendant unreasonably delayed in notifying Plaintiff and Class Members of the data breach until approximately June of 2022, despite having discovered the breach in December of 2021 when they were contacted by unknown third-party hackers who claimed responsibility for the data breach and who demanded money in exchange for the return of the stolen data.[3]

7. Even more egregiously, Defendant's Data Breach Notice sent to Plaintiff makes false claims and omits key information about the data breach. The Notice sent to Plaintiff claims MCG they did not discover the data breach until March 25, 2022, when in fact MCG actually discovered the breach in December of 2021.[4] Further, the Notice sent to Plaintiff also omits that MCG's own forensic investigators confirmed that hackers had already listed several stolen patient records for sale on the dark web.[5] Indeed, MCG's Notice is noticeably terse as to any details regarding the data breach, belying an intent on MCG's part to obfuscate

[3] *Notice of a Data Security Incident*, UNC Lenoir Health Care, https://www.unclenoir.org/app/files/public/eee43670-ad21-4614-b09989661edd7166/pdf-lenoirLEN%20PR%201017_Substitute%20Notice_6.13.2022%20FINAL.pdf (last visited July 28, 2022).

[4] *Id.*

[5] *Id.*

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

the true extent of the data breach. MCG's delay in timely notification, along with its efforts to downplay the severity of the data breach and has exacerbated the harm done to Plaintiff and Class Members.

8. As a result of MCG's wrongful actions and inactions, patient information was stolen. Plaintiff and Class Members who have had their PII compromised by nefarious third-party hackers, have had their privacy rights violated, have been exposed to the risk of fraud and identify theft, and have otherwise suffered damages. Plaintiff and Class Members bring this action to secure redress against MCG.

THE PARTIES

9. Plaintiff Tiffany Taylor is a California resident residing in Victorville, California. Plaintiff is a former patient of Desert Valley Hospital, who is a customer of MCG. On or around June 20, 2022, Plaintiff received a data breach notice from MCG informing her that her personal information, including her name, social security number, medical code, postal address, telephone number, email address, date of birth and gender, had been implicated in the data breach.

10. Defendant MCG Health, LLC is a Washington limited liability company with its principal place of business at 300 West 57th Street, New York, NY 10019. MCG's registered agent for service of process is CT Corporation System, who is located at 330 N. Brand Blvd., Ste. 700, Glendale, CA 91203.

11. Plaintiff is unaware of the true names, identities, and capacities of the defendants sued herein as DOES 1to 100. Plaintiff will seek leave to amend this Complaint to allege the true names and capacities of DOES 1 to 100 if and when ascertained. Plaintiff is informed and believes, and based thereon alleges, that each of the defendants sued herein as a DOE is legally responsible in some manner for the events and happenings alleged herein and that each of the defendants sued herein as a DOE proximately caused injuries and damages to Plaintiff and Class members as set forth below.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

JURISDICTION AND VENUE

12. T This Court has subject matter jurisdiction over the state law claims asserted herein pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), since Plaintiff is a citizen of a State different from the Defendant and, upon the original filing of this complaint, members of the putative Plaintiff class resided in states around the country; there are more than 100 putative class members; and the amount in controversy exceeds $5 million.

13. The Court also has personal jurisdiction over the Parties because Defendant routinely conducts business in California and has sufficient minimum contacts in California to have intentionally availed themselves to this jurisdiction by marketing and selling their technology services in California.

14. Venue is proper in this District because, among other things: (a) Plaintiff Tiffany Taylor is a resident of this District and a citizen of this state; (b) Defendant directed its activities at residents in this District; and (c) many of the acts and omissions that give rise to this Action took place in this judicial District for reservations in this district.

15. Venue is further appropriate in this District pursuant to 28 U.S.C. § 1391 because, among other things: (a) Plaintiff resides in the Central District, (b) Defendant conducts substantial business in the Central District, (c) Defendants directed their services at residents in the Central District; and (d) many of the acts and omissions that give rise to this Action took place in the Central District.

FACTUAL ALLEGATIONS

A. The Data Breach

16. MCG is a HIPAA business associate that provides informed care strategies and clinical guidance software to hospitals and healthcare providers using artificial intelligence technology. In providing it's services, MCG collects and stores patient PII and PHI from its customers. As a result, MCG's systems store the

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

PII and PHI of millions of patients from hospitals and healthcare providers from across the United States.

17. On or around December of 2021, MCG's systems were accessed by unauthorized third-party hackers, who exfiltrated Plaintiff's and Class Members' sensitive PII and PHI—including, but not limited to, their names, social security numbers, medical codes, postal addresses, telephone numbers, email addresses, dates of birth and gender. In its data breach notification filed the United States Secretary of Health and Human Services, MCG reported that the data breach had affected 793,283 individuals.[6] However, in its data breach notification filed with the Office of the Maine Attorney General, MCG reported that the total affected number of individuals may be as high as 1,100,000.[7]

18. Following this data breach, MCG was contacted by the hackers, who made a demand for money in exchange for the return of the stolen patient data.[8] At or around this time, MCG's forensic investigators confirmed that the PII/PHI of several affected individuals had been already posted for sale on the dark web by the hackers.[9]

B. Defendant's Unreasonably Delayed and Inadequate Notification

19. MCG owed Plaintiff and Class Members a duty under state and federal law to provide timely notification of the data breach. Under Cal. Civ. Code §1798.82(a), MCG was required to provide such notification "in the most expedient time possible and without unreasonable delay." Likewise, MCG was also required

[6] *Cases Currently Under Investigation*, U.S. Department of Health and Human Services, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited July 28, 2022).
[7] *Data Breach Notifications*, Office of the Maine Attorney General, https://apps.web. maine.gov/online/aeviewer/ME/40/ 1948d82a-0cdb-4b37-a988-b4189351176b.shtml (last visited July 28, 2022).
[8] *Notice of a Data Security Incident*, UNC Lenoir Health Care, https://www.unclenoir.org/app/files/public/eee43670-ad21-4614-b09989661edd7166/pdf-lenoirLEN%20PR%201017_Substitute%20Notice_6.13.2022%20FINAL.pdf (last visited July 28, 2022).
[9] *Id.*

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

under 45 CFR §164.404(b) to provide such notification "without unreasonable delay and in no case later than 60 calendar days after discovery of a breach."

20. In its Data Breach Notice sent to Plaintiff, MCG claims that it discovered the data breach on or around March 25, 2022. However, MCG did not begin notifying Plaintiff and Class Members until on or around June of 2022, at least 68 days later.

21. Further, a Notice of Security Incident posted by UNC Lenoir Health Care, a customer and third-party business partner of MCG, reveals that MCG actually discovered the data breach in December of 2021.[10] Thus, MCG in fact delayed an approximate total of *seven* months in notifying Plaintiff and Class Members of the data breach. There can be no question that MCG's notification was unreasonably delayed.

22. The Data Breach Notice sent to Plaintiff also withholds multiple key details regarding the data breach—including that third-party criminal hackers had already posted the PII/PHI of several affected individuals for sale on the dark web. Indeed, MCG's Data Breach Notice contains very little details on any kind, belying an intent to obfuscate the full extent of the data breach. MCG's omissions have impeded Plaintiff and Class Members from learning the true extent of the data breach, as well as the true risk of financial and identity fraud that MCG had placed them in.

C. MCG's Failure to Provide Reasonable, Adequate, and Compliant Data Security

23. MCG's privacy policy promises that it will use "reasonable efforts to protect your information" using "a variety of security technologies and procedures to protect information from unauthorized access, use or disclosure."[11]

[10] *Id.*

[11] *Privacy Policy*, MCG, https://www.mcg.com/privacy-policy/ (last visited July 28, 2022).

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

24. MCG clearly recognized its duty to provide reasonable data security for Plaintiff's and Class Members' PII/PHI that it collects and stores as part of its business practices. MCG made promises to do so. Despite this, on information and belief, MCG did not implement reasonable data security safeguards and protocols to protect Plaintiff's and Class Members PII/PHI.

D. MCG's Obligation to Protect Patient PII/PHI Under State and Federal Law

25. Under §1798.81.5(b) of the California Customer Records Act, MCG was required to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

26. As a HIPAA business associate, MCG holds a statutory duty under HIPAA and other federal and state statutes to safeguard Plaintiff's and Class Member's PII/PHI.

27. Under the HIPAA Privacy Rule, MCG is required to:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives maintains or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by their workforce.

45 CFR §164. 306(a)

28. The HIPAA Privacy Rule also requires MCG to "review and modify the security measures implemented…as needed to continue provision of reasonable and appropriate protection of electronic protected health information" under 45

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

C.F.R. §164.306(e) and to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights" under 45 C.F.R. §164.312(a)(1).

29. Further, the Federal Trade Commission Act, 45 U.S.C. §45 prohibits MCG from engaging in "unfair or deceptive acts or practices affecting commerce." The Federal Trade Commission has found The Federal Trade Commission has found that a company's failure to maintain reasonable and appropriate data security for the consumers' sensitive personal information is an "unfair practice" in violation of the Federal Trade Commission Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 243 (3rd Cir. 2015).

30. MCG failed to comply with each of these state and federal statutes by failing to implement and maintain reasonable security procedures to protect Plaintiff and Class Members' PII/PHI.

E. Applicable Standards of Care

31. In addition to their obligations under state and federal law, MCG owed a duty to Plaintiff and the Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PII in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. MCG owed a duty to Plaintiff and the Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer system and networks, and the personnel responsible for them, adequately protected the PII of Plaintiff and Class Members.

32. MCG owed a duty to Plaintiff and the Class Members to design, maintain, and test their computer system to ensure that the PII in Defendants' possession was adequately secured and protected.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

33. MCG owed a duty to Plaintiff and the Class Members to create and implement reasonable data security practices and procedures to protect the PII in their possession, including adequately training their employees and others who accessed the PII in their possession, including adequately training their employees and others who accessed PII in their computer systems on how to adequately protect PII.

34. MCG owed a duty of care to Plaintiff and Class Members to implement processes that would detect a breach of their data security systems in a timely manner.

35. MCG owed a duty to Plaintiff and the Class Members to act upon data security warnings and alerts in a timely fashion.

36. MCG owed a duty to Plaintiff and Class Members to disclose if their computer systems and data security practices were inadequate to safeguard individuals' PII/PHI from theft because such an inadequacy would be a material fact in the decision to provide or entrust their PII/PHI to MCG.

37. MCG owed a duty to Plaintiff and the Class Members to disclose in a timely and accurate manner when the data breach occurred.

38. MCG owed a duty of care to Plaintiff and the Class Members because they were foreseeable and probable victims of any inadequate data security practices. MCG received PII/PHI from Plaintiff and Class Members with the understanding that Plaintiff and Class Members expected their PHI/PII to be protected from disclosure. Defendants knew that a breach of its data systems would cause Plaintiff and Class Members to incur damages.

F. Stolen Information Is Valuable to Hackers and Thieves

39. It is well known, and the subject of many media reports, that PII/PHI is highly coveted and a frequent target of hackers. Especially in the technology industry, the issue of data security and threats thereto is well known. Despite well-publicized litigation and frequent public announcements of data breaches,

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

Defendant opted to maintain an insufficient and inadequate system to protect the PII/PHI of Plaintiff and Class Members.

40. Plaintiff and Class Members value their PII/PHI, as in today's electronic-centric world, their PII/PHI is required for numerous activities, such as new registrations to websites, or opening a new bank account, as well as signing up for special deals.

41. Legitimate organizations and criminal underground alike recognize the value of PII/PHI. That is why they aggressively seek and pay for it.

42. PII is highly valuable to hackers. Identity thieves use stolen PII for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. PII that is stolen from the point of sale are known as "dumps." *See All About Fraud: How Crooks Get the CVV*, Krebs on Security (April 26, 2016), https://krebsonsecurity.com/2016/04/all-about-fraud-how-crooks-get-the-cvv/.

43. Once someone buys PII/PHI, it is then used to gain access to different areas of the victim's digital life, including bank accounts, social media, and credit card details. During that process, other sensitive data may be harvested from the victim's accounts, as well as from those belonging to family, friends, and colleagues.

44. In addition to PII/PHI, a hacked email account can be very valuable to cyber criminals. Since most online accounts require an email address not only as a username, but also as a way to verify accounts and reset passwords, a hacked email account could open up a number of other accounts to an attacker.[12]

///

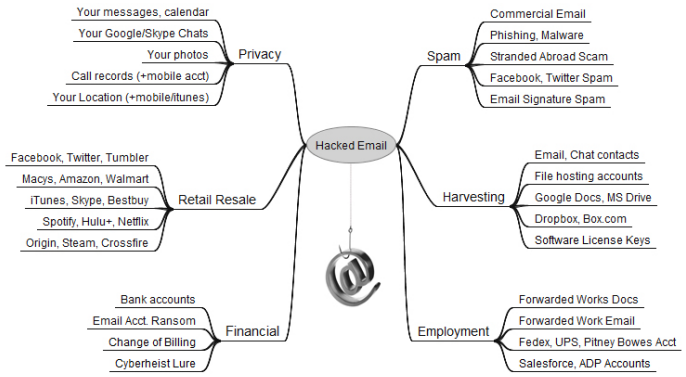
///

///

[12] *Identity Theft and the Value of Your Personal Data*, Trend Micro (Apr. 30, 2015), https://www.trendmicro.com/vinfo/us/security/news/online-privacy/identity-theft-and-the-value-of-your-personal-data.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

45. As shown below, a hacked email account can be used to link to many other sources of information for an identity thief, including any purchase or account information found in the hacked email account.[13]



46. Hacked information can also enable thieves to obtain other personal information through "phishing." According to the Report on Phishing available on the United States, Department of Justice's website: "AT&T, a large telecommunications company, had its sales system hacked into, resulting in stolen order information including full names and home addresses, order numbers and credit card numbers. The hackers then sent each customer a highly personalized e-mail indicating that there had been a problem processing their order and re-directing them to a spoofed website where they were prompted to enter further information, including birthdates and Social Security numbers."[14]

///

///

///

[13] Brian Krebs, *The Value of a Hacked Email Account*, Krebs on Security (June 13, 2013, 3:14 PM), https://krebsonsecurity.com/2013/06/the-value-of-a-hacked-email-account/.

[14] *Report on Phishing* (Oct. 2006), https://www.justice.gov/archive/opa/docs/report_on_phishing.pdf

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

G. The Data Breach Has and Will Result in Additional Identity Theft and Identity Fraud

47. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to protect the PII of Plaintiff and the Class Members. The ramification of Defendant's failure to keep Plaintiff and the Class Members' data secure is severe.

48. Between 2005 and 2019, at least 249 million individuals were affected by health care data breaches.[15] In 2019 alone, over 505 data HIPAA data breaches were reported, resulting in over 41 million healthcare records being exposed, stolen, or unlawfully disclosed.[16]

49. It is incorrect to assume that reimbursing a consumer for a financial loss due to fraud makes that individual whole again. On the contrary, after conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems." *See Victims of Identity Theft*, U.S. Department of Justice (Dec 2013), https://www.bjs.gov/content/pub/pdf/vit12.pdf. In fact, the BJS reported, "resolving the problems caused by identity theft [could] take more than a year for some victims." *Id*.

H. Annual Monetary Losses from Identity Theft are in the Billions of Dollars

50. Javelin Strategy and Research reports that losses from identity theft reached $21 billion in 2013. There may be a time lag between when harm occurs and when it is discovered, and also between when PII is stolen and when it is used.

[15] *Healthcare Data Breaches: Insights and Implications*, National Library of Medicine (May 13, 2020), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133.

[16] *December 2019 Healthcare Data Breach*, HIPAA Journal, https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO, Report to Congressional Requesters (June 2007), http://www.gao.gov/new.items/d07737.pdf.

51. This is particularly the case with HIPAA data breaches such as MCG's, as the information implicated, such as social security numbers of medical history, cannot be changed. Once such information is breached, malicious actors can continue misusing the stolen information for years to come. Indeed, medical identity theft are one of the most common, most expensive, and most difficult-to-prevent forms of identity theft.[17] Victims of medical identity theft "often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[18]

52. Indeed, a study by Experian found that the average total cost of medical identity theft is "nearly $13,500" per incident, and that many victims were forced to pay out-of-pocket costs for fraudulent medical care.[19] Victims of healthcare data breaches often find themselves "being denied care, coverage or reimbursement by their medical insurers, having their policies canceled or having

[17] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare* (Feb. 7, 2014), https://khn.org/news/rise-of-indentity-theft/.
[18] *Id.*
[19] *Healthcare Data Breach: What to Know About them and What to Do After One*, EXPERIAN (June 14, 2018), https://www.experian.com/blogs/ask-experian/healthcare -data-breach-what-to-know-about-them-and-what-to-do-after-one/.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores."[20]

53. Plaintiff and the Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any financial or identity fraud they suffer.

I. Plaintiff and Class Members Suffered Damages

54. The exposure of Plaintiff and Class Members' PII/PHI to unauthorized third-party hackers was a direct and proximate result of Defendants' failure to properly safeguard and protect Plaintiff and Class Members' PII from unauthorized access, use, and disclosure, as required by and state and federal law. The data breach was also a result of Defendant's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff and Class Members' PII in order to protect against reasonably foreseeable threats to the security or integrity of such information, also required by their contracts and state and federal law.

55. Plaintiff and Class Members' PII/PHI is private and sensitive in nature and was inadequately protected by Defendants. Defendants did not obtain Plaintiff and Class Members' consent to disclose their PII, except to certain persons not relevant to this action, as required by applicable law and industry standards.

56. As a direct and proximate result of Defendant's wrongful actions and inaction and the resulting data breach, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing risk of harm from identity theft and identity fraud, requiring them to take the time and effort to mitigate the actual and potential impact of the subject data breach on their lives by, among other things, paying for credit and identity monitoring services, spending time on credit and identity monitoring, placing "freezes" and "alerts" with credit reporting agencies,

[20] *Id.*

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

contacting their personal, financial and healthcare institutions, closing or modifying personal, financial or healthcare accounts, and closely reviewing and monitoring their credit reports, financial accounts and healthcare accounts for unauthorized activity.

57. Plaintiff has also lost the value of her PII/PHI. PII/PHI is a valuable commodity, as evidenced by numerous companies which purchase PII from consumers, such as UBDI, which allows its users to link applications like Spotify, Twitter, or Apple Health and opt-in to paid opportunities to earn income, and Brave, which uses a similar business model, and by market-based pricing data involving the sale of stolen PII across multiple different illicit websites.

58. Top10VPN, a secure network provider, has compiled pricing information for stolen PII, including $160.15 for online banking details, $35.00 for credit reports, and $62.61 for passports. Standalone Yahoo email accounts have been listed for as little as $0.41, while banking logins are in the range of $500, and verified Paypal accounts with high balances are listed at as much as $2,000.

59. In addition, Privacy Affairs, a cyber security research firm, has listed the following prices for stolen PII:

U.S. driving license, high quality:	$550
Auto insurance card:	$70
AAA emergency road service membership card:	$70
Wells Fargo bank statement:	$25
Wells Fargo bank statement with transactions:	$80
Rutgers State University student ID:	$70

60. Defendants' wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff and Class Members' PII/PHI, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

a. The improper disclosure and theft of their PII/PHI;

b. The imminent and impending injury flowing from potential fraud and identity theft posed by their PII/PHI being exposed to and misused by unauthorized third-party hackers;

c. The untimely and inadequate notification of the data breach;

d. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the data breach; and

e. Ascertainable losses in the form of deprivation of the value of their PII/PHI, for which there is a well-established national and international market.

CLASS ACTION ALLEGATIONS

61. Plaintiff brings this action on their own behalf and pursuant to the Federal Rules of Civil Procedure Rule 23(a), (b)(2), (b)(3), and (c)(4). Plaintiff intends to seek certification of a Nationwide Class and California Subclass. The Classes are initially defined as follows:

The Nationwide Class, initially defined as:

> All persons residing in the United States of America who received a data breach notice informing them that their PII/PHI had been breached by unauthorized third parties as a result of MCG's data breach.

The California Sub-Class, initially defined as:

> All persons residing in the State of California who received a data breach notice informing them that their PII/PHI had been breached by unauthorized third parties as a result of MCG's data breach.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

62. Excluded from each of the above Classes is Defendant, including any entity in which Defendant has a controlling interest, is a parent or subsidiary, or which is controlled by Defendant, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendant. Also excluded are the judge and the court personnel in this case and any members of their immediate families. Plaintiff reserves the right to amend the Class definitions if discovery and further investigation reveal that the Classes should be expanded or otherwise modified.

63. *Numerosity*, Fed. R. Civ. P. 23(a)(1): The members of the Classes are so numerous that the joinder of all members is impractical. The disposition of the claims of Class Members in a single action will provide substantial benefits to all parties and to the Court. The Class Members are readily identifiable from information and records in Defendant's possession, custody, or control, such as reservation receipts and confirmations.

64. *Commonality*, Fed. R. Civ. P. 23(a)(2) and (b)(3): There are questions of law and fact common to the Classes, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant took reasonable steps and measures to safeguard Plaintiff's and Class Members' PII;
b. Whether Defendant violated common and statutory by failing to implement reasonable security procedures and practices;
c. Which security procedures and which data-breach notification procedure should Defendant be required to implement as part of any injunctive relief ordered by the Court;
d. Whether Defendant knew or should have known of the security breach prior to the disclosure;

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

e. Whether Defendant has complied with any implied contractual obligation to use reasonable security measures;

f. Whether Defendant's acts and omissions described herein give rise to a claim of negligence;

g. Whether Defendant knew or should have known of the security breach prior to its disclosure;

h. Whether Defendant had a duty to promptly notify Plaintiff and Class Members that their PII was, or potentially could be, compromised;

i. What security measures, if any, must be implemented by Defendant to comply with its duties under state and federal law;

j. The nature of the relief, including equitable relief, to which Plaintiff and the Class Members are entitled; and

k. Whether Plaintiff and the Class Members are entitled to damages, civil penalties, and/or injunctive relief.

65. *Typicality*. Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because Plaintiff's PHI/PII, like that of every other Class Member, was misused and/or disclosed by Defendant.

66. *Adequacy of Representation*, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the members of the Classes. Plaintiff has retained competent counsel experienced in litigation of class actions, including consumer and data breach class actions, and Plaintiff intends to prosecute this action vigorously. Plaintiff's claims are typical of the claims of other members of the Classes and Plaintiff has the same non-conflicting interests as the other Class Members. Therefore, the interests of the Classes will be fairly and adequately represented by Plaintiff and her counsel.

67. *Superiority of Class Action*, Fed. R. Civ. P. 23(b)(3): A class action is superior to other available methods for the fair and efficient adjudication of this

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

controversy since joinder of all the members of the Classes is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

68. Damages for any individual class member are likely insufficient to justify the cost of individual litigation so that, in the absence of class treatment, Defendant's violations of law inflicting substantial damages in the aggregate would go un-remedied.

69. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2), because Defendant has acted or refused to act on grounds generally applicable to the Classes, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Classes as a whole.

CAUSES OF ACTION

FIRST CAUSE OF ACTION

Negligence

(On Behalf of Plaintiff and the Nationwide Class)

70. Plaintiff repeats and incorporates herein by reference each and every allegation contained in paragraphs 1 through 69, inclusive, of this Complaint as if set forth fully herein.

71. In 2016, the Federal Trade Commission ("FTC") updated its publication, "Protecting Personal Information: A Guide for Business," which establishes guidelines for fundamental data security principles and practices for business. [21] Among other things, the guidelines dictate businesses should protect any personal customer information that they keep; properly dispose of personal

[21] Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personalinformation.pdf.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses implement an intrusion detection system to expose breaches as soon as they occur; monitor all incoming traffic for activity indicating someone is attempting to infiltrate or hack the system; monitor instances when large amounts of data are transmitted to or from the system; and have a response plan ready in the event of a breach. [22] Additionally, the FTC recommends that companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures. [23]

72. Defendant owed Plaintiff and the Class Members a duty of care in the handling of customers' PII. This duty included, but was not limited to, keeping that PII secure and preventing disclosure of the PII to any unauthorized third parties. This duty of care existed independently of Defendants' contractual duties to Plaintiff and the Class Members. Under the FTC Guidelines, and other sources of industry-wide cybersecurity standards, Defendant is obligated to incorporate adequate measures to safeguard and protect PII that is entrusted to them in their ordinary course of business and transactions with customers.

73. Pursuant to the Federal Trade Commission Act (15 U. S. C. §45), Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff and Class Members' PII. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, treating the businesses' failure to employ

[22] *Id.*

[23] Federal Trade Commission, *Start With Security: A Guide for Business* (Jun. 2015) https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U. S. C. § 45. Orders from these actions further clarify the measures businesses are required to undertake in order to satisfy their data security obligations. [24]

74. Additional industry guidelines which provide a standard of care can be found in the National Institute of Standards and Technology's ("NIST's") *Framework for Improving Critical Infrastructure Cybersecurity* (Apr. 16, 2018), https://nvlpubs. nist. gov/nistpubs/CSWP/ NIST. CSWP. 04162018. pdf. Among other guideposts, the NIST's framework identifies seven steps for establishing or improving a cybersecurity program (section 3. 2). Those steps are:

> *Step 1: Prioritize and Scope*. The organization identifies its business/mission objectives and high-level organizational priorities. With this information, the organization makes strategic decisions regarding cybersecurity implementations and determines the scope of systems and assets that support the selected business line or process. The Framework can be adapted to support the different business lines or processes within an organization, which may have different business needs and associated risk tolerance. Risk tolerances may be reflected in a target Implementation Tier.
>
> *Step 2: Orient*. Once the scope of the cybersecurity program has been determined for the business line or process, the organization identifies related systems and assets, regulatory requirements, and overall risk approach. The organization then consults sources to identify threats and vulnerabilities applicable to those systems and

[24] Federal Trade Commission, *Privacy and Security Enforcement: Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-securityenforcement (last visited Nov. 22, 2019).

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

assets.

Step 3: Create a Current Profile. The organization develops a Current Profile by indicating which Category and Subcategory outcomes from the Framework Core are currently being achieved. If an outcome is partially achieved, noting this fact will help support subsequent steps by providing baseline information.

Step 4: Conduct a Risk Assessment. This assessment could be guided by the organization's overall risk management process or previous risk assessment activities. The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. It is important that organizations identify emerging risks and use cyber threat information from internal and external sources to gain a better understanding of the likelihood and impact of cybersecurity events.

Step 5: Create a Target Profile. The organization creates a Target Profile that focuses on the assessment of the Framework Categories and Subcategories describing the organization's desired cybersecurity outcomes. Organizations also may develop their own additional Categories and Subcategories to account for unique organizational risks. The organization may also consider influences and requirements of external stakeholders such as sector entities, customers, and business partners when creating a Target Profile. The Target Profile should appropriately reflect criteria within the target Implementation Tier.

Step 6: Determine, Analyze, and Prioritize Gaps. The organization compares the Current Profile and the Target Profile to determine gaps. Next, it creates a prioritized action plan to address

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

gaps – reflecting mission drivers, costs and benefits, and risks – to achieve the outcomes in the Target Profile. The organization then determines resources, including funding and workforce, necessary to address the gaps. Using Profiles in this manner encourages the organization to make informed decisions about cybersecurity activities, supports risk management, and enables the organization to perform cost-effective, targeted improvements.

Step 7: Implement Action Plan. The organization determines which actions to take to address the gaps, if any, identified in the previous step and then adjusts its current cybersecurity practices in order to achieve the Target Profile. For further guidance, the Framework identifies example Informative References regarding the Categories and Subcategories, but organizations should determine which standards, guidelines, and practices, including those that are sector specific, work best for their needs.

75. In addition to their obligations under federal regulations and industry standards, Defendant owed a duty to Plaintiff and the Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiff and the Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer systems and networks, and the personnel responsible for them, adequately protected the PII/PHI of Plaintiff and the Class Members.

76. Defendants owed a duty to Plaintiff and the Class Members to design, maintain, and test their internal data systems to ensure that the PII in Defendant's possession was adequately secured and protected.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

77. Defendants owed a duty to Plaintiff and the Class Members to create and implement reasonable data security practices and procedures to protect the PII in its custodianship, including adequately training its employees and others who accessed PII within its computer systems on how to adequately protect PII.

78. Defendant owed a duty to Plaintiff and the Class Members to implement processes or safeguards that would detect a breach of their data security systems in a timely manner.

79. Defendant owed a duty to Plaintiff and the Class Members to act upon data security warnings and alerts in a timely fashion.

80. Defendant owed a duty to Plaintiff and the Class Members to timely disclose if its computer systems and data security practices were inadequate to safeguard individuals' PII from theft because such an inadequacy would be a material consideration in Plaintiff and Class Members' decisions to entrust their PHI/PII to Defendants.

81. Defendant owed a duty to Plaintiff and the Class Members to disclose in a timely and accurate manner when data breaches occur.

82. Defendant owed a duty of care to Plaintiff and the Class Members because they were foreseeable and probable victims of any inadequate data security practices and systems. Defendant collected PII from Plaintiff and the Class Members. Defendants knew that a breach of its data systems would cause Plaintiff and the Class Members to incur damages.

83. Defendants breached its duties of care to safeguard and protect the PII which Plaintiff and the Class Members entrusted to it. Defendant adopted inadequate safeguards to protect the PII and failed to adopt industry-wide standards set forth above in its supposed protection of the PII. Defendant failed to design, maintain, and test its computer system to ensure that the PII was adequately secured and protected, failed to create and implement reasonable data security practices and procedures, failed to implement processes that would detect a breach of its data

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

security systems in a timely manner, failed to disclose the breach to potentially affected customers in a timely and comprehensive manner, and otherwise breached each of the above duties of care by implementing careless security procedures which led directly to the breach.

84. Defendant breached the duties set forth in 15 U.S.C. §45, the FTC guidelines, the NIST's Framework for Improving Critical Infrastructure Cybersecurity, and other industry guidelines. In violation of 15 U.S.C. §45, Defendant failed to implement proper data security procedures to adequately and reasonably protect Plaintiff and Class Member's PII/PHI. In violation of the FTC guidelines, *inter alia*, Defendant did not protect the personal customer information that it keeps; failed to properly dispose of personal information that was no longer needed; failed to encrypt information stored on computer networks; lacked the requisite understanding of their network's vulnerabilities; and failed to implement policies to correct security problems. In violation of the NIST's Framework, Defendant, *inter alia*, failed to adopt sufficient resources to identity and address security gaps.

85. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

86. As a direct and proximate result of Defendant's failure to adequately protect and safeguard the PII, Plaintiff and the Class members suffered damages. Plaintiff and the Class Members were damaged because their PII was accessed by third parties, resulting in increased risk of identity theft, property theft and extortion for which Plaintiff and the Class members were forced to adopt preventive and remedial efforts. These damages were magnified by the passage of time because Defendant failed to notify Plaintiff and Class Members of the data breach until weeks had passed. In addition, Plaintiff and Class Members were also damaged in that they must now spend copious amounts of time combing through their records in order to ensure that they do not become the victims of fraud and/or identity theft.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

87. Plaintiff and Class Members have suffered actual injury and are entitled to damages in an amount to be proven at trial but in excess of the minimum jurisdictional requirement of this Court.

SECOND CAUSE OF ACTION

Violation of the California Customer Records Act,

Cal. Civil Code § 1798. 80 *et seq.* ("CCRA")

(On Behalf of Plaintiff and the California Sub-Class)

88. Plaintiff repeats and incorporates herein by reference each and every allegation contained in paragraphs 1 through 87, inclusive, of this Complaint as if set forth fully herein.

89. Cal. Civ. Code §1798.81.5(b) requires that "[a] business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

90. Plaintiff and the Class Members are "customer[s]" within the meaning of Cal. Civil Code §1798.80(c) and are California residents.

91. Defendant is a "business" within the meaning of Cal. Civil Code §1798. 80(a).

92. Plaintiff and the Class Members' PII constitutes "personal information" within the meaning of Cal. Civil Code § 1798.80(e).

93. Defendant violated Cal. Civ. Code § 1798.81.5(b) by failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect Plaintiff and the Class Members' PII from unauthorized access, destruction, use, modification, or disclosure as evidenced by the fact that the security of Plaintiff and the Class Members' PII was compromised and exposed to at least one unauthorized party and perhaps more.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

94. As a direct and proximate result of Defendant's violation of Cal. Civ. Code §1798.81.5(b), Plaintiff and the Class Members' PII was compromised and exposed in connection with the data breach.

95. Cal. Civ. Code §1798.82(a) requires that "[a] person that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data…in the most expedient time possible and without unreasonable delay."

96. Defendant unreasonably delayed in notifying Plaintiff and Class Members of the data breach. Defendant discovered the data breach in December of 2021. However, Defendant did not begin notifying Plaintiff and Class Members of the data breach until on around June of 2022, a delay of roughly seven months.

97. As a result of the data breach and the exposure of their PII to unauthorized third parties, Plaintiff and the Class Members have been placed at an imminent, immediate, and continuing risk of identity theft-related harm and are thereby entitled to recover compensatory damages in an amount according to proof at trial pursuant to Cal. Civ. Code §1798.84(b).

THIRD CAUSE OF ACTION

Violation of the California Consumer Privacy Act,

Cal. Civ. Code § 1798. 150 *et seq* ("CCPA")

(On Behalf of Plaintiff and the California Sub-Class)

98. Plaintiff repeats and incorporates by reference each and every allegation contained in paragraphs 1 through 97 inclusive of this Complaint as if set forth fully herein.

///

///

///

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

99. Under Cal. Civ. Code § 1798.150(a)(1),

> (a)(1) Any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:
>
> (A) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater.
>
> (B) Injunctive or declaratory relief.
>
> (C) Any other relief the court deems proper.

Cal. Civ. Code § 1798.150(a)(1).

100. Plaintiff and the Class Members provided to Defendant their nonencrypted and nonredacted personal information as defined in § 1798.81.5 in the form of their PII/PHI. This PII/PHI included their names, social security numbers, medical codes, street addresses, telephone numbers, email addresses, dates of birth and genders.

101. Plaintiff and the Class Members' PII was subject to unauthorized access and exfiltration when it was exposed to and harvested by hackers.

102. The unauthorized access, exfiltration, theft, and disclosure of Plaintiff and the Class Members' PII was a result of Defendant's violation of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

103. Under Defendant's duty to protect customers' PII, it was required to implement reasonable security measures to prevent and deter hacks from accessing the PII of its customers. That these vulnerabilities existed and enabled unauthorized third parties to access and harvest customers PII evidence that Defendant has breached that duty.

104. Plaintiff and Class Members have suffered actual injury and are entitled to damages in an amount to be proven at trial but in excess of the minimum jurisdictional requirement of this Court.

105. Under the CCPA's "notice and cure" provision, Plaintiff is required to provide Defendants with written notice at least 30 days prior to the commencement of an action identifying the specific provisions Plaintiff alleges have been or are being violated. In satisfaction of this requirement, Plaintiff will send written notice to Defendants via certified or registered mail contemporaneously with the filing of this Complaint. Plaintiff's written notice is attached hereto as **Exhibit A**. Plaintiff will seek to amend the Complaint to seek relief once the requisite 30-day notice period has expired and to state that Plaintiff gave Defendants proper notice.

FOURTH CAUSE OF ACTION

Violation of the Confidentiality of Medical Information Act,

Cal. Civ. Code § 56 *et seq* ("CMIA")

(On behalf of Plaintiff and the California Sub-Class)

106. Plaintiff repeats and incorporates by reference each and every allegation contained in paragraphs 1 through 105 inclusive of this Complaint as if set forth fully herein.

107. Defendant, as a "business organized for the purpose of maintaining medical information in order to make the information available to an individual or provider of health care…" is a "provider of health care" under Cal. Civ Code §56.06 and is thus subject to the CMIA.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

108. Plaintiff and Class Members are "patients" under Cal. Civ. Code §56.06(j).

109. Defendant, as a direct result of its unlawful actions and inactions, disclosed "medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization" by allowing third-party criminal hackers to access and exfiltrate Plaintiff and Class Members' PHI/PII in violation of Cal. Civ. Code §56.10(a). In doing so, Defendant breached the confidentiality of Plaintiff and Class Members' protected information in violation of Cal. Civ. Code §56.101(a) by allowing unauthorized persons to view Plaintiff and Class Member's PII/PHI.

110. Plaintiff and Class Members have suffered actual injury and are entitled to damages under Cal. Civ. Code §56.35 and §56.36 in an amount to be proven at trial but in excess of the minimum jurisdictional requirement of this Court.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all of the Class Members, respectfully requests that the Court enter judgment in her favor and against Defendant as follows:

1. For an Order certifying the Classes as defined herein and appointing Plaintiff and her Counsel to represent the Classes;
2. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;
3. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety and to disclose with specificity to Class Members the type of PII compromised.
4. For an award of actual damages, statutory damages and compensatory damages, in an amount to be determined at trial;
5. For an award of punitive and treble damages, in an amount to be determined at trial;
6. For an award of costs of suit, litigation expenses and attorneys' fees, as allowable by law; and
7. For such other and further relief as this Court may deem just and proper.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of herself and all others similarly situated, hereby demands a jury trial for all claims so triable.

Dated: July 26, 2022

Respectfully Submitted,

/s/ *Thiago M. Coelho*
Thiago M. Coelho
WILSHIRE LAW FIRM, PLC
Attorneys for Plaintiff

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137